FILED ENTERED
LOGGED RECEIVED
JAN 27 2020
AT BALTIMORE
CLERK, U.S. DISTRICT COURT
DISTRICT OF MARYLAND
BY DEPUTY

20-0290 TMD

20-0291 TMD 20-0292 TMD

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A CRIMINAL COMPLAINT AND SEARCH WARRANTS

I, Special Agent Michael Stearns of the United States Secret Service, being first duly sworn, state the following:

INTRODUCTION AND AGENT BACKGROUND

1. I submit this affidavit in support of a criminal complaint and arrest warrant for Juliet CERVELLON, charging her with a criminal violations of 18 U.S.C. § 656 (Theft, Embezzlement, or Misapplication by Bank Officer or Employee) and 18 U.S.C. § 1028A (Aggravated Identify Theft) (the "SUBJECT OFFENSES").

2. I also make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search and seizure warrant to search the person of CERVELLON (further described in Attachment A-1) and the residence located at 72 Spa Road, Annapolis, MD (further described in Attachment A-2) to seize evidence, fruits, and instrumentalities of the SUBJECT OFFENSES (further described in Attachment B). I am an "investigative or law enforcement officer of the United States" within the meaning of Rule 41(a) of the Federal Rules of Criminal Procedure and am authorized to make applications for search and seizure warrants and to serve arrest warrants.

3. I am a duly appointed Special Agent with the United States Secret Service ("USSS") and have been employed as such since June 2017. Through my employment with the USSS, I have gained knowledge in the use of various investigative techniques including the utilization of physical surveillance, undercover agents, confidential informants and cooperating witnesses, consensually monitored recordings, investigative interviews, financial investigations, the service of administrative and grand jury subpoenas, mobile wireless tracking methods,

MJS 1/24/2020

analyzing telephone pen register and caller identification system data, and the execution of search and arrest warrants, including those executed upon physical addresses as well as those executed upon electronic equipment and data storage providers.

4. Throughout my career in law enforcement, I have become familiar with the methods and techniques associated with financial institution fraud and counterfeit trends and tactics. In the course of conducting financial investigations, I have incorporated the use of the following investigative techniques: interviewing informants, cooperating witnesses, victims, and subjects; physical surveillance and utilization of various surveillance techniques; supporting undercover operations; participating in mobile wireless tracking missions; and preparing and executing search and arrest warrants that have led to seizures of counterfeit currency, access devices, and other instruments used to commit financial fraud.

5. Based on my knowledge, training, and experience in the investigation of financial institution fraud, I am familiar with the ways in which fraudsters conduct their business. My familiarity includes the various means and methods by which individuals defraud financial institutions; their use of cellular telephones and social media accounts to facilitate fraud; and their use of code words to describe fraud. I am familiar with the ways that those who commit financial institution fraud are able to carry out their fraud without detection. Financial institution fraud is commonly an ongoing and recurring criminal activity. As contrasted with crimes against persons, which tend to be discrete offenses, crimes such as bank fraud and wire fraud are illicit commercial activities that are characterized by regular, repeated criminal activity.

6. Based on my training and experience, I know that individuals engaged in financial institution fraud and identity theft typically store evidence of their criminal activity on their persons, in their residences, and in their vehicles. I know that such persons typically retain copies

TMD

TMD 1/24/2020

of fraudulent documents and materials so that they are readily accessible for use. Such documents and materials may include stolen and/or fraudulent identification documents, checks, credit and debit cards; documents and materials containing personal identifying information ("PII") of individual victims; and documents and materials reflecting shipments and transmissions of victims' PII and fraudulent and/or stolen documents and materials. Participants in financial institution fraud and identity theft schemes also carry on their persons, in their residences, and in their vehicles their own genuine credit and debit cards and other documents and materials identifying financial accounts in which the proceeds of their fraudulent activities may be stored or traced.

7. In addition, I know from my training and experience that individuals engaged in financial institution fraud and identity theft often carry mobile electronic storage devices (including cell phones) on their persons and in their vehicles, or keep them in their residences, and use such devices and device features (including photos, voice calls, text messages, and emails) to store information and to communicate with others in furtherance of their crimes. Such individuals commonly use and maintain within their residences personal computers also used to store information and to communicate with others in furtherance of their crimes. Computers, cell phones, and other electronic storage devices allow participants in financial fraud and identity theft schemes to transmit compromised identity and financial information, and to conduct transactions and other activities in furtherance of their fraud schemes across substantial distances. Data obtained from computers, cell phones, and other electronic storage devices of those involved in financial fraud and identity theft (such as email and social media accounts, contacts, call logs, location data, and photos) has enabled law enforcement to identify co-conspirators. Computers, cell phones, and other electronic storage devices also commonly contain indicia of ownership and

TMP

MHP 1/27/2020

information identifying users of the devices. The foregoing information is commonly maintained within the electronic storage device for substantial periods of time, to include several months and even years, at little or no cost. Files from computers and mobile electronic devices, or remnants of such files, can be recovered months or even years after they have been saved in an electronic storage medium, deleted, or viewed via the Internet.

8. Based on the evidence gathered to date, there is probable cause to believe that Juliet Cervellon ("CERVELLON") has committed the SUBJECT OFFENSES and that evidence, fruits, and instrumentalities of the SUBJECT OFFENSES, further described in Attachment B, may be found on the person of CERVELLON and within the SUBJECT PREMISES, further described in Attachments A-1 and A-2, respectively, including any electronic storage devices found within those locations.

9. Because this Affidavit is being submitted for the limited purpose of establishing probable cause for an arrest warrant and search warrants, I have not included every detail of every aspect of the investigation. Rather, I have set forth only those facts that I believe are necessary to establish probable cause. However, I have not excluded any information known to me that would defeat a determination of probable cause. The information contained in this Affidavit is based upon my personal knowledge, my review of documents and other evidence, and my conversations with other law enforcement officers and other individuals.

PROBABLE CAUSE

10. Juliet CERVELLON ("CERVELLON") is a resident of Annapolis, Maryland, formerly employed by Wells Fargo as a branch manager. Investigation into conduct by CERVELLON revealed that she used her position with Wells Fargo to gain access to customers' bank accounts and obtained at least approximately $320,000 through fraud between August 2012

TMP

mrp 1/24/2020

and November 2018. Wells Fargo is a financial institution whose deposits are insured by the Federal Deposit Insurance Corporation.

11. A Wells Fargo customer with the initials A.O. contacted Wells Fargo on May 1, 2017, to report fraud on her accounts. A.O. stated that she possessed only one valid debit card and never requested or ordered additional debit cards. Information obtained from Wells Fargo revealed that 19 debit cards were connected to accounts opened in A.O.'s name and that some of the cards were mailed to the Wells Fargo branch located at 930 Bay Ridge Rd., Annapolis, MD (the "Bay Ridge Road Branch") without A.O.'s authorization. CERVELLON worked at the Bay Ridge Road Branch as branch manager between December 2013 and January 2017, having previously worked at the Wells Fargo branch located at 171 Jennifer Rd., Annapolis, Maryland (the "Jennifer Road Branch") beginning in October 2010.

12. Wells Fargo and A.O., over the course of multiple interviews with law enforcement and Wells Fargo fraud investigators, provided the following information: A.O. first met CERVELLON while CERVELLON was employed at the Jennifer Road Branch. Due to a cultural connection, CERVELLON befriended A.O. and utilized her banking experience and ability to speak Spanish to gain the trust of A.O. A.O. continued her banking relationship with CERVELLON when CERVELLON moved to the Bay Ridge Road Branch as a branch manager. When A.O. came into the branch to conduct transactions, CERVELLON would immediately provide assistance. During the course of the banking relationship, CERVELLON was able to access account information pertaining to A.O. and circumvent banking procedures in order to obtain financial records. A substantial portion of deposits into A.O.'s accounts consisted of rental payments for rental properties she owned and were made through CERVELLON at Wells Fargo branches. A.O. did not utilize online banking with any of her accounts and never asked for receipts after making deposits because she believed that CERVELLON was competently managing her

MTP 1/27/2020

accounts. A.O. monitored the accounts by calling or visiting the Wells Fargo branch and speaking directly with CERVELLON.

13. Between September 28, 2011, and December 28, 2016, 19 different debit cards were ordered from the Wells Fargo accounts opened in A.O.'s name. Some of the cards were sent directly to the Bay Ridge Road Branch, to the attention of Juliet CERVELLON, and activated in the branch by CERVELLON. Based on Wells Fargo internal audits, CERVELLON created PIN codes for at least some of the debit cards for use in transactions. Between 2014 and 2017, a total of approximately $320,000 was debited from A.O.'s accounts through debit card transactions at ATMs and via retail purchases that A.O. did not authorize.

14. The debit cards were used in transactions at multiple businesses to include: Lorena Auto Repair, Griffith Energy, Maryland Oral Surgery, Dental One, Victoria's Secret, Fitzergald's Auto, Baltimore Gas and Electric, Justice, and multiple other businesses in Anne Arundel and Prince George's Counties, Maryland, as well as travel to New York, New Jersey, and Virginia. A.O. stated that she does not shop at any merchants where the cards were used, does not commonly use debit cards, and pays utility bills only by check. Business records indicate that CERVELLON regularly visited the above mentioned businesses for vehicle repairs, to purchase clothes, or for medical appointments, and used her own identification cards to pay for services at times. On several occasions between January 2015 and January 2017, debit cards associated with accounts in A.O.'s name were used to make utility payments to Griffith Energy for an account in CERVELLON's name and for service to her residential address, 72 Spa Road, Annapolis, MD (the "SUBJECT PREMISES"). On June 15, 2016, a debit card was used at Fitzergald's Auto in Annapolis, MD to pay approximately $992.76 for service on a Cadillac Escalade vehicle registered to CERVELLON. The debit cards were also used to make payments through the Internet to

MMP 1/24/2020

telecommunications service provider Verizon, credit card company Capital One, and online payments processor Paypal. The online payments to Capital One were payments on a credit card in CERVELLON's name. I know through training and experience that these types of online payments are made using Internet-connected computers and mobile electronic devices, such as cell phones.

15. According to information provided by Wells Fargo, CERVELLON went on maternity leave in 2015. Maternity-related expenditures (such as obstetrician's office visits and purchases from maternity clothing and baby stores) paid using debit cards fraudulently issued in A.O.'s name began occurring on or about March 8, 2015, and ended on or about May 17, 2015. The debit cards were not used to make purchases between May 18, 2015, and November 14, 2015. While on maternity leave, CERVELLON was away from work and may have lacked access to A.O.'s account, which may explain the lack of spending during this period of time. Web search results of CERVELLON's name through Google populates results including CERVELLON's baby registry with Babies R Us, which provides an estimated due date of September 23, 2015. Fraudulent purchases resumed on or about November 15, 2015. Purchases at children's clothing and toy stores such as Gymboree, Carter's, and the Disney store continued to be made in 2016 using debit cards associated with accounts held in A.O.'s name.

16. On December 16, 2016, CERVELLON was captured in video surveillance at an ATM located at the Bay Ridge Branch in Annapolis, MD withdrawing funds from A.O.'s account 0779 with one of the debit cards issued without A.O.'s authorization. A still image from the video surveillance footage is displayed below:

MP 1/27/2020

17. On January 5, 2019, Wells Fargo customer with the initials P.P. contacted Anne Arundel County Police Department to file a report that two fraudulent checks were drawn on an account held by his sister C.P., each in the amount of $9,500.00. P.P. held power of attorney of the account. P.P. advised that neither he nor C.P. authorized the checks to be written and did not order any new checks for the account. According to information provided by Wells Fargo, the checks were sent and mailed to the Bay Ridge Road Branch. Check no. 378 is dated November 23, 2018, and was negotiated on November 27, 2018, at a branch of Bank of America located in Annapolis, MD. Check no. 431 is dated October 17, 2018, and was negotiated on October 18, 2018, at a Bank of America branch located in Annapolis, MD. Each of the checks was made payable to an individual with the initials R.G.P., and the memo line of each check refers to "child support." Wells Fargo security indicated that the handwriting on each check appears to be similar to CERVELLON's handwriting.

18. CERVELLON's primary residence is a single-family home located at 72 Spa Road, Annapolis, MD, further described in Attachment A-2 (the "SUBJECT PREMISES").

mvp 1/24/2020

CERVELLON resides at the SUBJECT PREMISES with her children. On August 7, 2019, I conducted surveillance of the SUBJECT PREMISES in order to verify that CERVELLON still resided at the SUBJECT PREMISES. I observed a Cadillac Escalade, bearing Maryland license plate 4CG8006, parked in the driveway for the SUBJECT PREMISES. The vehicle is registered to CERVELLON and is the same vehicle referenced above in Paragraph 14. Additionally, Annapolis Police Department responded to the SUBJECT PREMISES on July 10, 2019, for a report of an assault and verified that CERVELLON resided at the location. On December 4, 2019, Annapolis Police Department detectives conducted a criminal investigation involving CERVELLON's daughter and verified that CERVELLON still resides at the SUBJECT PREMISES.

CONCLUSION

21. Based on the foregoing, I submit that there is probable cause to believe that Juliet CERVELLON has committed violations of 18 U.S.C. § 656 (Theft, Embezzlement, or Misapplication by Bank Officer or Employee) and 18 U.S.C. § 1028A (Aggravated Identify Theft), and that evidence, fruits, and instrumentalities of the foregoing offenses (further described in Attachment B) may be found on CERVELLON's person (further described in Attachment A-1) and in the SUBJECT PREMISES (further described in Attachment A-2).

WHEREFORE, in consideration of the facts presented, I respectfully request that this Court issue an arrest warrant for Juliet Cervellon and the requested search warrants.

Michael Stearns
Special Agent
United States Secret Service

20-0291 TMD 20-0292 TMD

Subscribed and sworn to before me this 24 day of January 2020. 20-0290 TMD

The Honorable Thomas M. DiGirolamo
United States Magistrate Judge
United States District Court for the District of Maryland

MR 1/24/2020

20-0291

ATTACHMENT A-1

DESCRIPTION OF PERSON TO BE SEARCHED

The person to be searched is:

Name: Juliet CERVELLON
DOB: XX/XX/1981
Gender: Female
Race: Hispanic
Height: 5'6"
Weight: 160 lbs.
Eyes: brown
Hair: brown

1/24/2020

20-0292 TMD

ATTACHMENT A-2

DESCRIPTION OF PREMISES TO BE SEARCHED

The premises to be searched is located at 72 Spa Road, Annapolis, Maryland, is the residence of Juliet Cervellon. The dwelling is a two-story, split-foyer, single-family house with a driveway. This residence has a back door on the basement level that opens into an open field behind the residence.

MR
1/27/20

20-0291 TMD 20-0292 TMD

ATTACHMENT B

ITEMS TO BE SEIZED

The items to be seized are evidence, fruits, information, contraband, or instrumentalities, in whatever form and however stored, relating to violations of 18 U.S.C. § 656 (Theft, Embezzlement, or Misapplication by Bank Officer or Employee)and 18 U.S.C. § 1028A (Aggravated Identify Theft), as described in the search warrant affidavit, including, but not limited to, the following:

a. Documents showing occupancy, use, residency, rental agreements, and/or ownership of the location being searched;

b. Any documents constituting or relating to any address book, diary, calendar, or listing of contact information of personal and/or business associates of Juliet CERVELLON, including any book, paper, log, or other item used to record or store names, addresses, telephone numbers, appointments, or events;

c. Any documents, materials, written communications or correspondence containing the personal identifying information of persons other than Juliet CERVELLON or any residents of the SUBJECT PREMISES, including any identification documents or cards, or copies thereof;

d. Any credit or debit cards, bank checks, receipts or invoices of transactions, and records or documents relating to the issuance, receipt, use, or distribution of any credit or debit cards or bank checks, including but not limited to, inventories, ledgers, journals, bank account or other financial statements, check registers, notes, and correspondence;

e. Any cash or currency of any kind that may be traceable to the above described offenses;

f. Any documents or materials referring or relating to the location of any cash or funds traceable to the above described offenses, including any keys to safes or safe deposit boxes;

g. Any door, safe, locked boxes, or receptacles where the aforementioned items may be hidden;

h. Any documents or materials containing computer passwords and information regarding data security devices necessary to gain access to any computer equipment or electronic storage devices seized during the search; and

i. Any computer hardware, mobile electronic storage device, or other electronic storage medium, including file servers, desktop computers, laptop computers, mainframe

MS 1/24/2020

20-0291 TMD 20-0292 TMD

computers, hard drives, zip drives, CD-ROMs, floppy disks, cellular telephones, flash drives, thumb drives, and any internal and external peripheral devices (e.g., printers, scanners);

For any computer or electronic storage medium whose seizure is otherwise authorized by this warrant, and any computer or electronic storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the COMPUTER was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the COMPUTER user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web

TMD

MV 1/24/2020

20-0291 TMD 20-0292 TMD

pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The law enforcement search shall be conducted pursuant to the following protocol in order to minimize to the greatest extent possible the likelihood that files or other information for which there is not probable cause to search are viewed.

With respect to the search of any digitally/electronically stored information provided to law enforcement by forensic analysis, the search procedure by law enforcement may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein, while permitting government examination of all the data necessary to determine whether that data falls within the items to be seized):

a. surveying various file directories and the individual files they contain to determine whether they include data falling within the list of items to be seized;

b. opening or reading portions of files in order to determine whether their contents fall within the items to be seized;

c. scanning storage areas to discover data falling within the list of items to be seized, to possibly recover any such deleted data, and to search for and recover files falling within the list of items to be seized; and/or

d. performing key word searches through all electronic storage areas to determine whether occurrence of language contained in such storage areas exist that are likely to appear in the evidence to be seized.

If after performing these procedures, the directories, files or storage areas do not reveal evidence of the above listed crimes or other criminal activity, the further search of that particular directory, file or storage area, shall cease.

TMD

TMA 1/27/2020